

ORIGINAL

Approved: *A. Sowlati*
 ADAM SOWLATI
 Assistant United States Attorney

Before: THE HONORABLE KATHARINE H. PARKER
 United States Magistrate Judge
 Southern District of New York

23 MAG 2048

- - - - -	X	
	:	
UNITED STATES OF AMERICA	:	23 Mag.
	:	
- v. -	:	RULE 5(c)(3)
	:	AFFIDAVIT
PAUL WILLIAMS ANTI,	:	
	:	
	:	
Defendant.	:	
	:	
- - - - -	X	

SOUTHERN DISTRICT OF NEW YORK, ss.:

Graham Klein, being duly sworn, deposes and says that he is a Special Agent with the United States Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI"), and charges as follows:

On or about February 28, 2023, the United States District Court for the Western District of Wisconsin issued a warrant for the arrest of "Paul Williams Anti" on violations of Title 18, United States Code, Section 1956(h). A copy of the warrant is attached hereto as Exhibit A and incorporated by reference herein.

I believe that PAUL WILLIAMS ANTI, the defendant, who was taken into the custody of HSI in the Southern District of New York on or about March 13, 2023, is the same individual as the "Paul Williams Anti" who is wanted by the United States District Court for the Western District of Wisconsin.

The bases for my knowledge and for the foregoing charge are, in part, as follows:

1. I am a Special Agent with HSI. This affidavit is based upon my personal participation in this matter, as well as on my conversations with other law enforcement officers and my

examination of documents, reports, and records. I have been personally involved in determining whether PAUL WILLIAMS ANTI, the defendant, is the same individual as the "Paul Williams Anti" named in the February 28, 2023 warrant from the United States District Court for the Western District of Wisconsin. Because this Affidavit is being submitted for the limited purpose of establishing the identity of the defendant, I have not included in this Affidavit each and every fact that I have learned. Where I report statements made by others, those statements are described in substance and in part unless otherwise noted.

2. Based on my review of documents from proceedings in the United States District Court for the Western District of Wisconsin, I know that, on or about February 28, 2023, the United States District Court for the Western District of Wisconsin issued a warrant for the arrest of "Paul Williams Anti" (the "Warrant"). The Warrant was issued on a charge of violations of Title 18, United States Code, Section 1956(h).

3. On or about March 13, 2023, at approximately 6:15 a.m., I participated in the arrest of PAUL WILLIAMS ANTI, the defendant, at his home in the Bronx, New York. Based on my participation in that arrest, I and have learned, in substance and in part, the following:

a. During the arrest, PAUL WILLIAMS ANTI, the defendant, identified himself as "Paul Williams Anti."

b. Based on law enforcement's comparison of the fingerprints taken of WILLIAMS ANTI during processing with the fingerprints listed in law enforcement databases as belonging to the "Paul Williams Anti" wanted in the Warrant, I believe them to be identical.

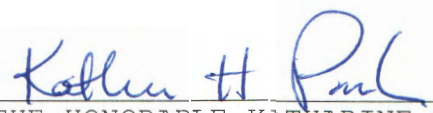
c. Upon the execution of a judicially authorized search warrant of the premises of WILLIAMS ANTI, I observed several identification documents that listed the identity of WILLIAMS ANTI as "Paul Kwasi Williams Anti."

WHEREFORE, I respectfully request that PAUL WILLIAMS ANTI, the defendant, be imprisoned or bailed, as the case may be.



Graham Klein
Special Agent
HSI

Sworn to before me this
14 day of March, 2023



THE HONORABLE KATHARINE H. PARKER
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA

v.

Case No.: 20-mj-134

PAUL WILLIAMS ANTI,

Defendant.

COMPLAINT FOR VIOLATION OF TITLE 18, UNITED STATES CODE, SECTION
1956(h)

BEFORE United States Magistrate Judge
Stephen L. Crocker

United States District Court
120 North Henry Street
Madison, Wisconsin 53703

The undersigned complainant being duly sworn states:

COUNT 1

1. From on or before October 13, 2020 to on or about October 20, 2020,
in the Western District of Wisconsin and elsewhere, the defendant,

PAUL WILLIAMS ANTI,

knowingly and intentionally conspired with others unknown to violate Title 18, United
States Code, Section 1956(a)(1)(B)(i). money laundering

2. Specifically, the defendant conspired with others to knowingly conduct
financial transactions affecting interstate commerce and foreign commerce, which
transactions involved the proceeds of specified unlawful activity, that is wire fraud,
knowing that the transactions were designed in whole or in part to conceal and disguise
the nature, location, source, ownership, and control of the proceeds of the specified

unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity.

3. Between on or about October 13, 2020, and on or about October 20, 2020, unknown fraud perpetrators used false pretenses to cause an employee of an organization in the Western District of Wisconsin (Organization A) to wire transfer the organization's funds to coconspirators including the defendant.

4. It was part of the conspiracy that defendant controlled the following bank accounts, each of which he opened using a false name and fraudulent identification information:

Bank Name	Fictitious Account Holder	Last Four of Account No.
Wells Fargo	G.P, dba Electronics General Goods	(0229)
Citizens Bank	G.P, dba Gary Ventures	(1157)

5. It was part of the conspiracy that on or before October 13, 2020, fraud perpetrators gained unauthorized access to the work email account of an employee of Organization A. Using their unauthorized access and without the employee's knowledge, fraud perpetrators obtained copies of incoming emails containing genuine invoices sent to the organization for payment. The fraud perpetrators altered the genuine invoices to increase the amounts due and changed where payment was to be directed.

6. It was further part of the conspiracy that, using their covert control over the employee's email account, fraud perpetrators sent emails containing the altered invoices to a second employee for payment. Not knowing the invoices had been altered and believing that the first employee had approved the invoices for payment, the second employee directed the organization's bank to wire funds to bank accounts actually controlled by the defendant and other coconspirators, in accordance with the altered invoice's payment instructions.

7. It was further part of the conspiracy that on October 19, 2020, after receiving an altered invoice with the fraudulent payee and balance due information, Organization A caused the invoice balance due of \$605,200 to be wire transferred from Organization A's bank account in Madison, Wisconsin, to the Wells Fargo account controlled by the defendant in the name of "G.P, dba Electronics General Goods" in Bloomfield, Connecticut.

8. It was further part of the conspiracy that once \$605,200 of Organization A's funds were wire transferred to the Wells Fargo account controlled by the defendant, the defendant, misrepresenting himself as "G.P," immediately conducted financial transactions to further direct some of fraud proceeds to other bank accounts he maintained under false identities. These accounts included another account in the name of "G.P, dba Gary Ventures," and an account in the name of "C.F. /Fowler Ventures."

9. During the time-period of the conspiracy, the defendant was employed as a health care worker under the false name K.A. The defendant directed mailings associated with his money laundering activities to the mailbox of an elderly patient he

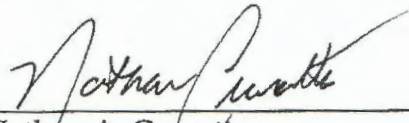
was caring for at a Connecticut nursing home. For example, defendant directed bank mailings associated with the two bank accounts named in paragraph 4 of the indictment to his patient's mailbox. The defendant retrieved the mailings when he picked up the patient's mail.

10. Of the approximately \$2.4 million in fraud derived proceeds, approximately \$1,000,000 was wired to the two bank accounts named in paragraph 4.

11. The defendant's actions were designed to conceal the source, control, ownership, and location of proceeds that were derived from a wire fraud-scheme. The defendant's actions were also designed to help conceal his true identity and avoid detection.

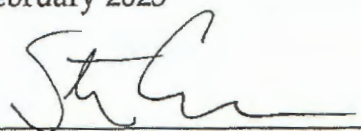
(All in violation of Title 18, United States Code, Section 1956(h)).

This complaint is based on the attached affidavit of Nathan A. Cravatta



Nathan A. Cravatta
Special Agent
Department of Homeland Security,
Homeland Security Investigations

Sworn to before me this 27th day of February 2023



HONORABLE STEPHEN L. CROCKER
United States Magistrate Judge

COUNTY OF DANE)
) ss
STATE OF WISCONSIN)

AFFIDAVIT

I, Nathan A. Cravatta, first being duly sworn under oath, hereby depose and state as follows:

1. I am a Special Agent with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and have been so employed since approximately May of 2005. My current job responsibilities include, but are not limited to, investigation of federal criminal laws involving financial fraud. In the past, I have been assigned to financial investigation groups that investigate bulk cash smuggling, money laundering offenses, and other fraud related offenses committed by criminal organizations. I have received formal training from the Federal Law Enforcement Training Center, as well as training through contact with experts from various law enforcement agencies.

2. I have received specialized training in federal financial crimes. I have participated in investigations involving large, international networks of individuals defrauding others using various electronic means, such as romance fraud-schemes, business email compromise schemes, and lottery schemes, etc. I have debriefed numerous victims of these schemes and reviewed large volumes of correspondence between victims and those perpetrating the frauds, as well as communications between co-schemers. I have also interviewed several defendants perpetrating these cyber-fraud schemes about, among other things, the methods by which victims are identified, the various roles individuals serve in the schemes, methods of communication, means of concealing identities, and the movement and concealment of fraud-derived funds. I

have also conducted physical and electronic surveillance, executed arrest and search warrants, acted in an undercover capacity, and analyzed electronic evidence, including the contents of numerous social media and email accounts controlled by individuals perpetrating fraud schemes.

3. The facts in this affidavit are known to me through my personal knowledge, training, experience, and through information provided to me by other law enforcement officers in the course of their official duties, whom I consider truthful and reliable. This affidavit is intended to show merely that there is sufficient probable cause for the complaint and does not set forth all of my knowledge about this matter.

4. The purpose of this affidavit is to establish probable cause that Paul K. Williams Anti has committed a violation of 18 U.S.C. § 1956(h) (money laundering conspiracy). Specifically, Williams Anti conspired with others to knowingly conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is wire fraud, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of the specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity.

5. I have used the general descriptions Organization A, Employee A, Employee B, and assisted living facility to protect the anonymity of the individuals and organizations who were victimized by the defendant's money laundering activities.

Similarly, rather than use the individual's names, I have referenced the individuals whose identities were misused by the defendant by their initials, G.P., C.F., and K.A.

6. On or about October 23, 2020, the Federal Bureau of Investigation (FBI) learned that Organization A, an organization headquartered in Madison, Wisconsin, lost approximately \$2.4 million because of a business email compromise scheme. The losses stemmed from Organization A paying invoices between approximately October 13, 2020 and October 20, 2020, later determined to have been altered.

7. FBI Special Agent Doug Raubal interviewed employees of Organization A. Those employees explained that the normal process for Organization A to receive and pay invoices from vendors was for Employee A to receive the invoices by email and then forward those emails to Employee B for payment. After learning of the fraud, both employees reviewed the payments in question and discovered the payment/wire information associated with the paid invoices had been altered. Many of the fraudulent invoices appeared to be from legitimate vendors with whom Organization A regularly conducted business, but the payee bank account information and sometimes the amount payable had been altered by an unknown party prior to being forwarded from Employee A to Employee B. This resulted in Organization A's funds being transferred into fraudulent bank accounts. Employee A reported she/he believed his work email account had been compromised.

8. Organization A provided SA Raubal with copies of the original, legitimate emails and associated invoices from their vendors, as well as copies of the fraudulent email chains and associated altered invoices which caused the fraudulent wire transfers to occur. SA Raubal also obtained, from the legitimate vendors, copies of the legitimate

email and invoices they sent to Organization A. By obtaining these emails SA Raubal was able to compare the original email/invoices to the fraudulent email/invoices. SA Raubal also examined forensically processed copies of the email boxes of Employee A and Employee B. Organization A's legitimate vendors also confirmed with SA Raubal that they did not send the altered invoices.

9. SA Raubal also obtained information from a private cyber-security company that Organization A hired to investigate the incident. The cyber-security company was unable to determine for certain how unknown persons gained access to Employee A's email account but did observe setting changes the unknown persons had made to the Employee A's account settings without Employee A's knowledge. The unknown fraud perpetrators changed the settings on Employee A's email account so any incoming emails that contained the words "invoice," "wire transfer," or "bank" would be automatically removed from the Employee A's email inbox and forwarded to a folder called "RSS Feeds." This made it less likely that Employee A would see the original emails containing the genuine invoices.

10. Using their access to Employee A's RSS Feeds file, fraud perpetrators retrieved the emails containing the original, legitimate invoices. They then altered the invoices to change payee bank account information, payment instructions, and invoice amounts. They then resent the altered invoices to Employee A from fraudulent email addresses made to look like vendor or Organization A email accounts. Using their control over Employee A's email account, fraud perpetrators forwarded the emails containing the altered invoices to Employee B. Not knowing the invoices had been altered and believing that the Employee A had approved the invoices for payment,

Employee B directed Organization A's bank to wire funds to bank accounts controlled by money laundering coconspirators like the defendant.

11. As part of the investigation, law enforcement obtained via subpoena, bank records associated with Organization A as well as bank records associated with the bank accounts where the fraud proceeds were wired. According to those records, on October 19, 2020, Organization A's bank wire transferred \$605,200 to a Wells Fargo account in Bloomfield, Connecticut, in the name of G.P., DBA Electronic General Goods (account number ending 0229). Bank records showed that the October 19, 2020 wire transfer from Organization A was quickly transferred out of this account by issuance of three checks, all purportedly signed by G.P. - a \$240,000 check issued to G.P, DBA Gary Ventures (deposited into a JP Morgan Chase business bank account); a \$180,000 check issued to C.F./Fowler Ventures (deposited into a Wells Fargo account); and a \$180,000 check issued to PTW Services LLC (deposited into a Bank of America account).

12. Then, on October 20, 2020, Organization A's bank wire transferred \$449,732.61 to a Citizens Bank account in the name of G.P., DBA Gary Ventures (account number ending 1157).

13. As detailed below, although the fraud proceeds were initially wired to bank accounts in the name of GP., the investigation has revealed that G.P. had nothing to do with any criminal activity. G.P.'s identity information was stolen by the defendant and used to open bank accounts used to receive and launder fraud proceeds. Defendant also compromised the identity of K.A. and C.F. to open bank accounts, conduct financial transactions, and facilitate his money laundering activities.

14. Both G.P. bank accounts had the same associated email address. On June 10, 2021, a search warrant was issued to Google LLC by the U.S. District Court for the Western District of Wisconsin for information related to the email account. Google LLC provided the requested records and those records showed the account was created on July 15, 2019 in the name of G.P. The account contained multiple emails showing the user of the email account creating other accounts and transferring money in the name of G.P. On August 25, 2020, the user received an email from Small World Money Transfer with the subject line of "Transaction MTN 2809650706" attaching a document labeled as "pre_transaction_2809650706.pdf." This document listed G.P. as the sender of \$700 to a person in Ghana. Small World Money Transfer also sent an email requesting the user's ID. In response, the user attached an image of a Connecticut driver's license in the name of G.P. I reviewed the image of that driver's license and compared it to the image of G.P.'s license from the Connecticut Department of Motor Vehicles. Virtually nothing about the purported Connecticut driver's license the email account user sent to Small World Money Transfer was consistent with the genuine license information for G.P. The subject in the above license was a different race, age, and had a different address and driver's license number than the real G.P. I confirmed with the Connecticut Department of Motor Vehicles that the driver's license number on this purported license did not exist in their system. The Connecticut Department of Motor Vehicles also told SA Raubal that this license was likely a counterfeit.

15. I also observed in the email account that the account user took numerous Uber rides to and from an assisted living facility in Connecticut. Mail for the G.P. bank

Case: 3:20-mj-00134-slc *SEALED* Document #: 21 Filed: 02/27/23 Page 11 of 13

accounts was also being directed – using a U.S. Postal Service auto-forwarding form – to Apartment 215 at that same address.

16. I reviewed records provided by the assisted living facility about the patient in Apartment 215, and those records showed that an individual named K.A. was the CNA caring for the elderly patient in that room. I interviewed the director of the assisted living facility about K.A. and she recounted a story in which a postal worker told her that he thought it was strange that the patient in room 215 was getting all sorts of mail addressed to other people. K.A., who picked up the patient's mail, was questioned and admitted he was having mail sent there, although he claimed it was mail for his family members.

17. I obtained and reviewed employment records for K.A. Among those records was a USCIS Form I-9, Employment Eligibility Verification Form. Attached to this form was a Permanent Resident Card bearing Alien Registration #A099-50x-xxx and an image of K.A. DHS database queries indicated this alien registration number is not assigned to K.A., so the Permanent Resident Card K.A. provided to his employer was fraudulent. I noted the photograph of K.A. was very similar to the photograph on the fraudulent G.P. driver's license.

18. As part of the investigation, SA Raubal requested the FBI's Criminal Justice Information Services, Face Services, attempt to identify the individual depicted on the counterfeit G.P. Connecticut driver's license using facial recognition software and various law enforcement databases. Facial analysis indicated the photo matched images associated with two individuals – one of the images was a visa application image for Paul Kwasi Williams Anti (DOB 10/28/xxx) (issued on May 8, 2012).

19. I reviewed DHS indices for Paul Kwasi Williams Anti. Images reviewed for Paul Kwasi Williams Anti in his alien registration file are consistent with the photo on the counterfeit G.P. driver's license and the image of K.A. from his employer. Williams-Anti is a native and citizen of Ghana. He has pending applications to U.S. Citizenship and Immigration Services (USCIS) to adjust his status.

20. On August 28, 2022, I located a Facebook account in the name of "Paul Kwasi Williams-Anti". Depicted on this account page was an image posted on November 24, 2021. This image was consistent with images I reviewed in Paul Kwasi Williams Anti's alien registration file, the photo on the counterfeit G.P. driver's license, and the image of K.A. In the photo depicted, Williams Anti is observed wearing a badge from the company that employed him under the name K.A.

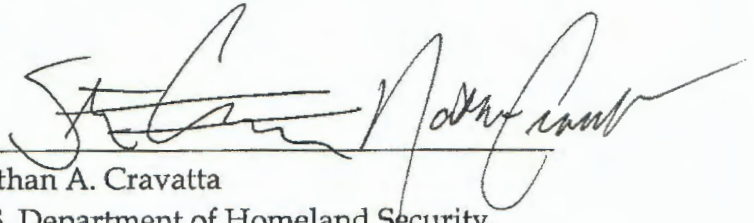
21. On December 15, 2022, a search warrant was issued to Apple, Inc. by the U.S. District Court for the Western District of Wisconsin for information related to the Apple ID williamsanti2012@gmail.com.

22. Records received indicate this account was created on August 11, 2016. Subscriber names listed for this account included Paul Kwasi Williams-Anti, Paul William, and K.A. Among the items recovered were images and documents associated with defendant's adjustment of status petition. Also recovered were images of numerous drivers licenses and social security cards in the names of real individuals but with defendant's photo. These included driver's licenses in the names of K.A., C.F., and G.P.

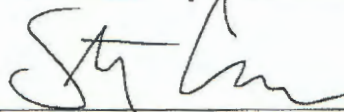
23. As discussed above, of the approximately \$2.4 million in fraud derived proceeds, approximately \$1,000,000 was wired to two bank accounts the defendant held

in the name of G.P. Then, using the identity of G.P., the defendant quickly transferred via check, the proceeds in one of the bank accounts to a third bank account the defendant held the name of G.P., a bank account the defendant held in the name of C.F./Fowler Ventures, and a bank account controlled by an unknown individual in the name of PTW Services LLC. The remaining \$1.4 million in fraud proceeds was wire transferred to two bank accounts controlled by individual(s) other than the defendant. Based on my review of the banking records associated with these accounts, these accounts were opened in fake names and the movement of money from those accounts is consistent with money laundering (ie., unexplained deposits followed by rapid smaller financial transactions to other individuals).

Dated this 27th day of February 2023


Nathan A. Cravatta
U.S. Department of Homeland Security,
Homeland Security Investigations

Sworn to this 27th day of February 2023.


STEPHEN L. CROCKER
United States Magistrate Judge